Strategy Research Project

Solving the Cross-Domain Conundrum

by

Colonel Bernard F. Koelsch
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
xx-03-2013	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Solving the Cross-Domain Conundrum

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Bernard F. Koelsch
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor William O. Waddell
Center for Strategic Leadership and Development

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5628

14. ABSTRACT

Commanders have operated in multiple security domains since the advent of national security classification structures and command and control systems. Planning, execution, and control in JIIM environments demands the movement of information between the security domains of all participants. Cross-domain solutions facilitate the necessary transfers, but only for systems designed to operate at multiple security levels or with multilevel security. Cross-domain solutions are also constrained by cost and security policies. Interoperability certification processes in the DOD components must require explicit identification of cross-domain requirements so the necessary resource flows are incorporated into system design. Multiple security level systems should expand their functions to provide cross-domain capability to commanders until multilevel security solutions become more prevalent and less costly. Capability developers should incorporate enterprise cross-domain services into objective architectures, in anticipation of DISA and DODIIS provisioning. Research and development efforts beyond the 2013 Future Years Defense Program should focus on domain convergence.

15. SUBJECT TERMS
Command and Control, Multilevel Security, Multiple Security Levels, Cross-Domain Solutions

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
UU	UU	UU	UU	36	

USAWC STRATEGY RESEARCH PROJECT

Solving the Cross-Domain Conundrum

by

Colonel Bernard F. Koelsch
United States Army

Professor William O. Waddell
Center for Strategic Leadership and Development
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Solving the Cross-Domain Conundrum
Report Date:	March 2013
Page Count:	36
Word Count:	5628
Key Terms:	Command and Control, Multilevel Security, Multiple Security Levels, Cross-Domain Solutions
Classification:	Unclassified

Commanders have operated in multiple security domains since the advent of national security classification structures and command and control systems. Planning, execution, and control in JIIM environments demands the movement of information between the security domains of all participants. Cross-domain solutions facilitate the necessary transfers, but only for systems designed to operate at multiple security levels or with multilevel security. Cross-domain solutions are also constrained by cost and security policies. Interoperability certification processes in the DOD components must require explicit identification of cross-domain requirements so the necessary resource flows are incorporated into system design. Multiple security level systems should expand their functions to provide cross-domain capability to commanders until multilevel security solutions become more prevalent and less costly. Capability developers should incorporate enterprise cross-domain services into objective architectures, in anticipation of DISA and DODIIS provisioning. Research and development efforts beyond the 2013 Future Years Defense Program should focus on domain convergence.

Solving the Cross-Domain Conundrum

In 2000, David Pearson authored a book that described the growing importance of Department of Defense (DOD) and Joint command and control (C2). He recognized that commanders at all levels need to collect a vast quantity of data, process it, and disseminate the resulting information. He further describes how inadequate the C2 systems were becoming:

> Networks are essential to performing the C2 mission. Data is distributed in enclaves, the boundaries of which are defined by security classification, user communities, and geographic locations. C2 systems have to provide personnel with access to the information they require, while denying them access to information for which they are not cleared. Task forces are assembling to study what hardware and software improvements are necessary to achieve such a capability. The governing council for the Department of Defense's global C2 system is gravely concerned about security. The council is developing interim means while working towards a multilevel computer security solution, an arrangement by which numerous users could access a system simultaneously and run programs at several classification levels. Throughout, the system would provide users with access to those types of information for which they had the appropriate security clearances while denying access to other information.[1]

Readers who work with C2 systems find this situation all too familiar. In fact, it has been familiar for users for almost 50 years. Pearson was not describing the current DOD C2 architecture shortfalls. He was depicting the automated data processing environment of 1965. The system was not today's Global Command and Control System (GCCS). It was its predecessor, the Worldwide Military Command and Control System (WWMCCS). The task force he refers to was formed by the Advanced Research Projects Agency (ARPA) in 1967. The group developing a way ahead for a multilevel security (MLS) capability was not a 21st century council of colonels. It was the WWMCCS Council of 1971. The promise of robust interoperability and secure access between security domains has eluded the best efforts of the defense community

since the Vietnam era. Today the cross-domain conundrum is still a major impediment to effective C2.

A Foot in Each Camp

It is not difficult to see the C2 challenges that result from having information segmented by classification. In 1970, WWMCCS terminated at the component command level and there were only two main information silos to contend with—operations and intelligence. Horizontal and vertical proliferation of networks and computing platforms in all joint capability areas forces commanders to have a foot in each camp.[2] Force application and C2 data are native to the Secure Internet Protocol Router Network (SIPRNet). Battlespace awareness data originates largely on the Joint Worldwide Intelligence Communications System (JWICS). Logistics data resides on Non-Classified Internet Protocol Router Network (NIPRNet). At the tactical, operational, and strategic levels, access to all three is a necessity.

Merely having access is not enough, however. Operational and strategic planning requires the fusion of multi-disciplinary information from data stores located in different security domains throughout the Defense enterprise. Processing data requires system access. Execution at the joint and component levels requires situational awareness and collaboration across the same security domains. Orders and instructions issued during point-to-point telephone calls secured with end-to-end encryption are relics of the past. C2 nodes communicate across data networks using chat, video teleconferencing, shared session collaborative tools, portals, and voice. The participants reside on disparate domains. We have long since exceeded the human capacity to fuse information and make decisions without some automated assistance or information technology intervention. The information has to move to a common

computing environment somehow. Seamless access to information will facilitate communication and understanding with mission partners and allow commanders to synthesize information more quickly and easily and create a decision advantage.[3]

Commanders and staffs cannot handle operations across two, three, or four domains even under optimal conditions. There are more camps to occupy than they have feet. Joint, interagency, intergovernmental, and multinational (JIIM) operations add security domains to the information architecture, raising the level of complexity well beyond anything imagined from the Cold War to Desert Storm. Coalition operations in Iraq and Afghanistan demonstrated the intricacy of managing multiple networks. International Security Assistance Forces (ISAF) created the Afghanistan Mission Network (AMN) as a core network for all forces, with extensions to other national networks such as the Combined Enterprise Regional Information Exchange System (CENTRIXS-ISAF), U.S. SIPRNet, UK OVERTASK, and State Department ClassNet at the Secret level.[4] Additionally, ISAF integrates information from other security domains at higher and lower levels (JWICS and NIPRNet). Without some kind of desktop reduction capability and cross-domain solutions (CDS), service members literally have piles of computer cases at their feet. Back at U.S. Central Command Headquarters, there are even more. The defense intelligence community plays security domain Twister® just like their operational counterparts. Top Secret/Sensitive Compartmented Information (TS/SCI) is spread among JWICS, Human Intelligence Operational Communications Network (HOCNet, Defense Intelligence Agency), NSANet (National Security Agency), Government Wide Area Network (GWAN, National Reconnaissance Office), and STONE GHOST (US-Australia-Canada-UK), to name a few.[5]

These enumerations highlight the scope and scale of the problems with information sharing across security domains for Coalition and Joint Force members. The challenges are not trivial. Staffs grow disproportionately and waste countless hours in dealing with cross-domain transfers, information exchanges, and distributed data management. At its worst, the situation diminishes the operational effectiveness of the force. Information must be shared with our U.S government and foreign military partners. The 9/11 Commission stated this need plainly: Action officers should be able to draw on all available knowledge in the government about a threat, and managers should ensure that information is shared and duties are clearly assigned across agencies, and across the foreign-domestic divide.[6] When CDS do not allow data access and consolidation, or when manual transfer procedures are restricted, or when the exchange between domains takes too long, what is a commander to do? Violate policy and regulations? In many cases, they do. Hopefully they make some responsible effort to adhere to information and physical security measures as they perform these *in extremis* acts of civil disobedience against cyber leadership. Shortfalls in cross-domain capability are legitimate conditions under which they have no reasonable choice.

To change these conditions and enable coherent access to information across many different domains, DOD should implement several short term solutions. First, and most importantly, capability developers must represent cross-domain requirements properly during system analysis and design. Second, interoperability certification must explicitly document cross-domain requirements in operational and system viewpoints. Third, existing systems with the most extensible cross-domain capabilities should be

grown and modularized to support expedient information exchanges. All three of these measures must support Command, Service, and Agency requirements as DOD, in conjunction with the Intelligence Community (IC), progresses towards the long-term goals of enterprise cross-domain services and domain convergence.

Short Term Solutions

System Design for Multi-Domain Operations

The biggest deficiency in cross-domain solutions is poor characterization of the requirements. Optimal system design is wholly dependent on effective system analysis. If the cross-domain requirements are not represented in the capability architecture, the participating systems will lack the requisite conditions for exchanges across security domain boundaries. A step-by-step examination of a generic C2 capability illustrates this.

System A (Figure 1) processes and displays tracking data for display within a common operational picture. It ingests event data from any number of sources and stores it in its database in a prescribed format. Subsystems process (P) and display (D) the event data, producing a view of the events that users observe at their workstation. In Figure 1, System A operates within one security domain (unclassified, in this example).

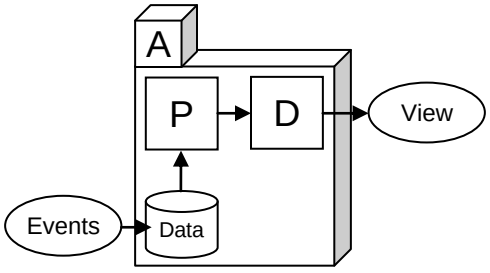

Figure 1. System in One Security Domain

To provide a common operational picture (COP) for both unclassified and classified networks, the organization deploys a second instance of the same system. System B has the same architecture as System A. Users access the unclassified COP on a NIPRNet workstation, and the classified COP on a SIPRNet workstation (Figure 2).

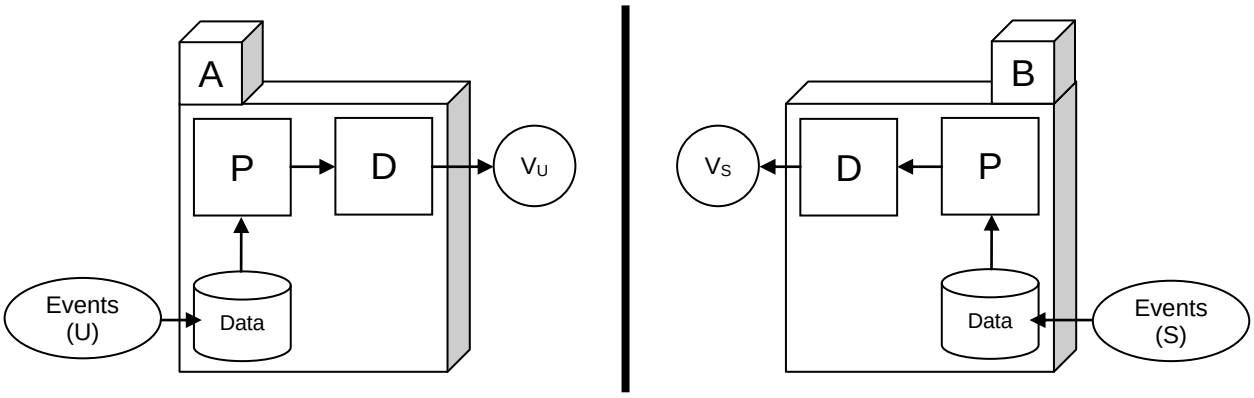

Figure 2. System in Two Security Domains

To view the unclassified and classified COPs on the same workstation, the organization can employ a multiple security level (MSL) capability. System C, which resides on the highest classified network, has trusted connections to other networks. System C does not process either COP, it merely brings a view of the System A and System B environments to a common display (Figure 3). Although the user at a System C workstation sees both the unclassified and classified COP on the same screen, they are still two separate views. The data is not integrated.

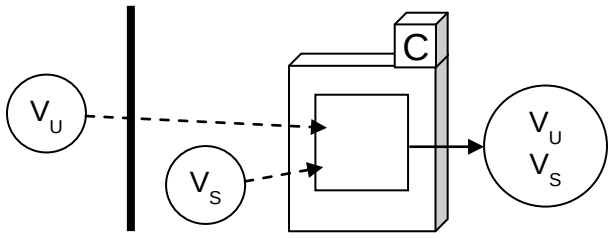

Figure 3. MSL View Consolidation

To integrate the unclassified and classified COP, the organization adds System G, a high assurance guard, to transfer unclassified data to System B (Figure 4). External capabilities that produce event data send it to System G in the appropriate format. System B adds Subsystem T, which transforms the data coming out of the guard into the schema needed to store, process, and display it. The result is a COP with unclassified and classified events integrated into the same view (V_{US}).

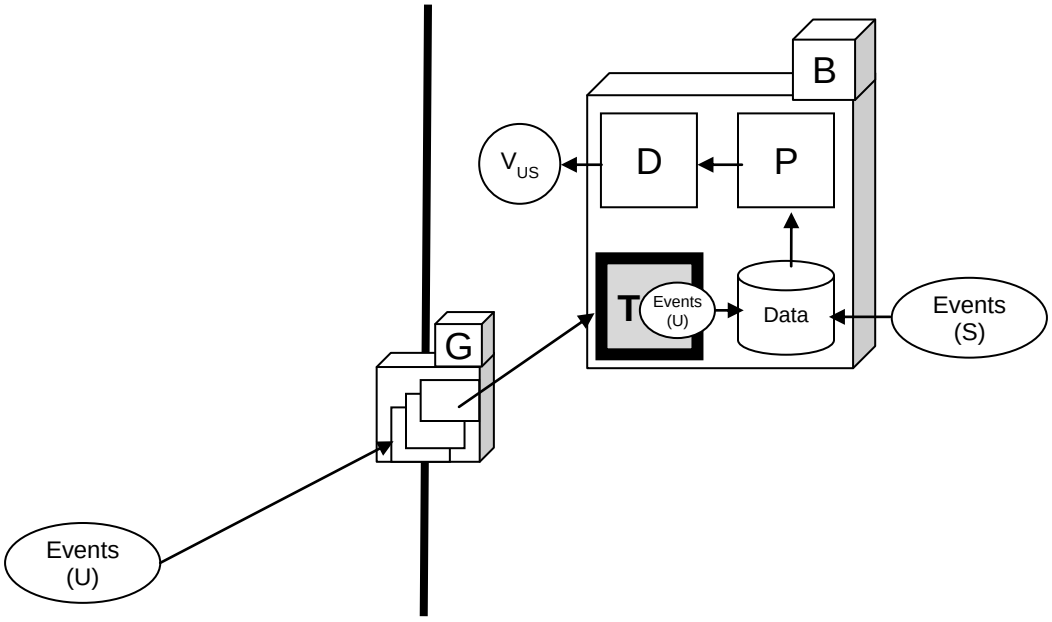

Figure 4. Upward Data Aggregation

Since the solution in Figure 4 does not provide an unclassified COP view to NIPRNet users, it is only acceptable if 1) other systems can provide event data to the guard without assistance from System B, and 2) the only view requirement is on the high network. Figure 5 depicts a more prevalent architecture for providing views at each level of security. Both Systems A and B incorporate transformation subsystems. In this multiple security level solution, users on both networks see a COP with events up to the level of security of their enclave.

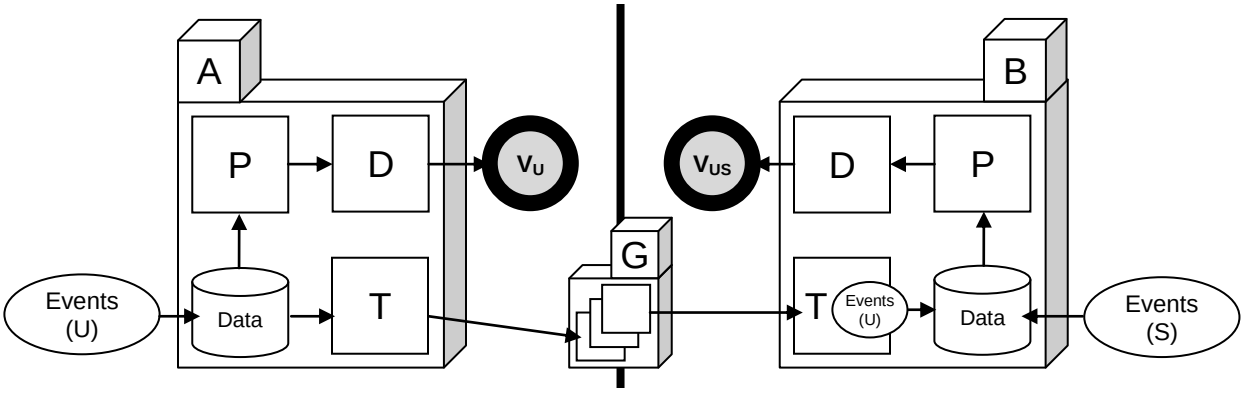

Figure 5. Vertical Data Distribution

Through simple operational viewpoints, this brief study demonstrates not only the level of complexity for typical CDS, but where else complexity lies. Although guards are complicated systems, they are not the panacea for effective information sharing among security domains. Capabilities must incorporate appropriate information exchanges to be interoperable among security domains. The resource flows that systems perform are a direct product of this modeling. In Figure 5, Systems A and B must work on common data standards, be able to securely deliver data to the guard in the right formats, and keep their various data stores synchronized. Without these considerations during system analysis and design, there is no hope of suitable capacity across boundaries, even with a flawless CDS between them. The less interoperable the design of the systems, the more capable the CDS must be. Systems fielded, updated or replaced without adequate considerations for JIIM environments contribute to the ever-widening gap between CDS performance and operational requirements.

True MLS capabilities close the gap because they integrate all aspects of the solution in the same processing environment. In Figure 6, events pass through controlled interfaces to the MLS system which labels all data in accordance with its

classification level. Through mandatory access controls and role-based access controls, the trusted operating system delivers users only the data they have access to. Guards within the subsystems ensure that the unclassified COP viewer sees only unclassified events, and classified COP viewers see all events at their authorized level and below. Other levels of stratification are possible, depending on the needs of the system.[7] For example, a vetted user from the United Kingdom might be authorized to see all COP events designated for release to Great Britain, the North Atlantic Treaty Organization (NATO), and U.S. Secret. A vetted user from France accessing the same COP data would only see NATO events.

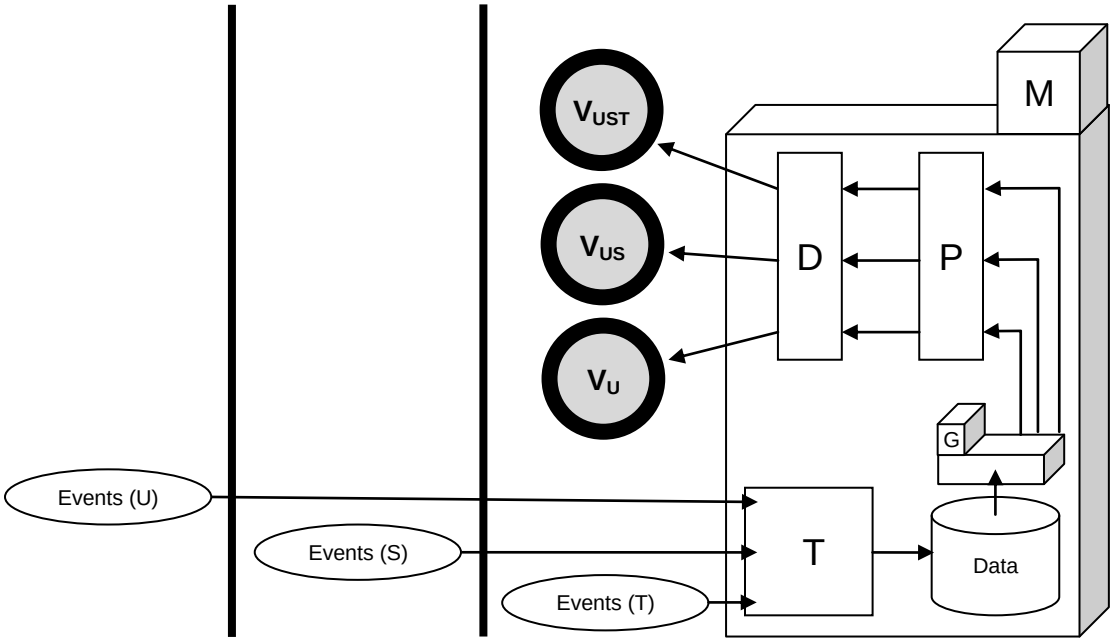

Figure 6. COP Views through MLS

This architecture has been successful in a few Service capabilities, but these achievements come at great cost. The data engineering required to consume the various data feeds from all the participating domains is immense. The price of secure network infrastructure and trusted computing environments is high. MLS solutions are

sound future investments for strategic and operational activities with at least semi-permanent facilities, adequate support staff, and user populations who perform complex, cross-discipline analysis. As a wholesale solution for commanders and staffs who need occasional access to the native trusted computing environment, MLS solutions are cost-prohibitive.

As the preceding examples demonstrate, the majority of specifications that conform a system to multi-domain operations exist not within the CDS, but within the overall C2 capability. If the operational viewpoints do not reflect a multi-domain operating environment, the resulting system analysis will not lead to a design that supports information sharing across security domain boundaries. CDS cannot, and should not, supply all the artifacts missing from the capability architecture. How data moves across the guards should be manifest in the standards viewpoints. The services viewpoint describes how the transfers occur, even when the CDS is outside of the core capability architecture. The data and information viewpoint establishes how the system will maintain integrity and consistency across all system instances in separate security domains.

Shortfalls in Interoperability Certification

Chairman of the Joint Chiefs of Staff Instruction 6212.01, which governs net ready key performance parameter (NR KPP) certification for joint capabilities, does not mandate declarations of cross-domain information exchanges between instances of the same system on different security domains. The Joint Staff must correct this deficiency to assure effective cross-domain functions in C2 capabilities. An initial capabilities document, capability development document or capability production document may appear to meet NR KPP requirements but the overall representation of the system can

deceptively omit the support necessary for synchronizing data and conducting transactions during simultaneous system operations in multiple, disparate security domains. Unless a capability has an inherent need to traverse security domain boundaries, program management will likely defer the requirement past initial operating capability or depend on an external service or capability to regulate the exchanges. The Automated Message Handling System (AMHS) is an example of a system with an inherent cross-domain requirement. AMHS delivers organizational record messages from one security domain to recipients on multiple security domains within requisite confidentiality, integrity, and availability.[8]

In system-of-system environments like GCCS, cross-domain requirements are more obscure. What systems have a cross-domain requirement? What systems will incorporate a CDS? What systems will rely on another system to conduct cross-domain exchanges? Having larger systems or centralized services provide such requirements for smaller systems is mutually beneficial to both in terms of simplicity and cost, but such dependencies should be formal. Consider the Joint Operation Planning and Execution System (JOPES) baseline within the GCCS family of systems. It would be inefficient for every subsystem of JOPES to integrate a CDS of its own. Subsystems format data in the United States Message Text Format (USMTF) based on Military Standard 6040[9] and GCCS message processors facilitate the transfers. Similarly, the GCCS global baseline forms the COP from track data transmitted across security domain boundaries in USMTF-mandated extensible markup language (XML) formats by tactical data systems.[10]

The operational view of a capability should articulate all of its related policies and procedures, and the system viewpoint models the resulting design (as defined by the Department of Defense Architecture Framework).[11] However, operational views persistently lack information exchanges that cross security domain boundaries, unless that exchange is with a different system. As a result, there are no associated resource flows in the systems viewpoint. The cascaded effect is gaps in the architecture across multiple viewpoints and insufficient system design. Data standards and models that support the best guard technologies available on the Unified Cross Domain Management Office Baseline List[12] are absent from the standards profile (StdV-1) and physical data model (DIV-3). The system meets the design parameters necessary for operation within one or more security domains but *it cannot interoperate with itself* between those instances. It becomes an island of excellence in the security domain sea. Getting to the sister islands is a problem deferred to the future. The consequence is finding suitable bridges and boats later—that is, finding a suitable CDS and adapting the capability infrastructure to support it.

Leading Service Efforts for Cross-Domain Interoperability

It is extremely difficult to extend existing system capability horizontally and vertically into other security domains. It is costly to convert existing data to common schemas. It is complex to create exchange services that can transform a wide variety of data sources into a format that high-speed guards can process. It is challenging to design systems that can detect and mitigate data inconsistencies among its own operating domains. With limited resources for new end-to-end system acquisitions, the Services must either adapt their existing systems or develop integrating capabilities to enable exchanges between the existing systems.

Army Intelligence took a system-high approach to improving cross domain intelligence and operational data exchanges with the Joint Intelligence Operations Capability – Iraq (JIOC-I). Fielded via the Distributed Common Ground System – Army (DCGS-A) version 2 in 2004,[13] it centralized operational and intelligence data at the TS/SCI level and established analytic functions at the core. Through controlled interfaces at varying levels of classification, consumers in different security domains could query for information and receive results trimmed to the limitations of their environment. Although this solution is highly dependent on the quality of data from numerous federated stores, it demonstrates an MLS solution with cross-domain information exchanges designated as critical interfaces in its original architecture.[14]

The Army Program Executive Office for Command, Control, and Communications-Tactical (PEO-C3T) has taken great strides towards cross-domain interoperability for units below the Corps level, but has not effectively bridged the gaps to joint, interagency, intergovernmental, and multinational domains. By 1999, standard elements in the Army Battle Command System (ABCS) common database allowed manifold information exchanges through the same common message processor used by the GCCS family of systems.[15] All the participating systems continued to operate only at the U.S. Secret level, which was sufficient for the leap-ahead capability ABCS gave to the First Digital Division in 2001[16] and to the 3rd Infantry Division during the invasion of Iraq in 2003. Tracking of assets outside the ABCS domain was accomplished sufficiently by one-way incoming feeds of global positioning satellite (GPS) location data from Blue Force Tracker devices. However, the specter of JIIM information exchanges loomed large in Iraq and Afghanistan. The Army Chief of Staff,

General Eric Shinseki, designated the “Top 7 Plus 1” operational needs for the PEO to expedite. The “Plus 1” was Joint and Coalition Interoperability. The implied cross-domain requirement of this mandate was addressed in ABCS version 6.4 in 2004. Data interoperability improved vastly in version 6.4 with the Publish and Subscribe Server (PASS) and its standard schemas. Nevertheless, the means to transfer the data remained unfulfilled.[17] In July 2006, the Iraq surge began to intensify interactions between Multi-National Force – Iraq (MNF-I) and Iraqi security forces. At the same time, the NATO assumed command in Afghanistan. Commanders were largely satisfied with their ability to command and control their own forces, but were clamoring for better means to exchange operational and intelligence information quickly and efficiently with their coalition partners. These needs remain unfulfilled as Iraq continues under Department of State oversight and Afghanistan draws down.

Systems such as the United States Marine Corps’ Command and Control PC (C2PC) are well suited to expand its cross-domain capability due to the flexibility of the C2PC Gateway architecture.[18] As C2PC and Army Force XXI Battle Command Brigade and Below converge into the Joint Battle Command – Platform, as instructed by Joint Requirements Oversight Council Memorandum 161-03,[19] the PASS architecture will provide COP data exchanges with other security domains for both Services.[20] PASS is also the connection point to Command Post of the Future (CPOF), which provides multi-echelon collaboration among similarly equipped operational units. CPOF is highly interoperable within the land component families of systems, yet still lacks the native design to achieve C2 exchanges across multiple security domains.[21]

The Navy's Ocean Surveillance Information System (OSIS) Evolutionary Development (OED) is an MLS solution with a systems architecture and logical data model similar to JIOC-I.[22] Originally fielded in shore-based joint and naval intelligence centers, it was adapted for afloat use on two fleet command and control ships: the USS Mount Whitney (Sixth Fleet and Commander Striking Force NATO) in 2001 and the USS Blue Ridge (Seventh Fleet) in 2003. OED not only mitigated the perpetual problem of space, power and cooling aboard the ships, it met a myriad of documented fleet requirements for cross-domain collaboration, multi-level intelligence production and dissemination, and all-security level message traffic and email management.[23]

The Air Force continues to leverage the cross-domain capabilities of GCCS-Joint for external information exchange requirements of the Air Operations Center – Weapon System. Specifically, they must ensure air mission planning and time-sensitive targeting data from Theater Battle Management Core System – Force Level (the Air Force instantiation of GCCS) is available through joint interfaces to fire and effect systems in other Service components.[24] Additionally, the Air Force Research Laboratory is the proponent for the Department of Defense Intelligence Information Systems (DoDIIS) Trusted Workstation (DTW), an MSL capability fielded to a number of key command centers including MNF-I, Marine Corps Intelligence Activity, U.S. Transportation Command, and the Office of the Under Secretary of Defense for Intelligence.[25] It allows single workstation access to any number of security domains by way of virtualization and remote session management. DTW, while not a MLS solution, included guard technologies that allow users to pass information between the domains in the background.[26]

Despite the best intentions to alleviate the shortfalls in C2, gaps between the security domains are still significant. Each Command, Service, and Agency is paving a road to a seamless MLS environment with good intentions, but the solutions never arrive in time to meet near-term requirements. The best way to enforce the necessary architectural approaches is to mandate the identification of multi-domain requirements in Joint Capabilities Integration Development System (JCIDS) documents. NR KPP attribute number 3, "must effectively exchange information,"[27] should explicitly require key performance parameters for cross-domain threads, if they exist or are projected to exist. Similar changes should be made to regulations that implement JCIDS within the Military Departments: Army Regulation 71-9, SECNAV Instruction 5000.2, and Air Force Instruction 10-601. Designing systems at the onset for cross-domain functions ensures that they will be interoperable with CDS interfaces and will reduce the complexity of CDS needed to perform transfers. This approach is most appropriate for C2 systems that use CDS to move large amounts of structured data with high throughput.

Creating an Expedient Cross-Domain Capability

For unstructured C2 data, commanders and staffs still require expedient means to move information between security domains quickly and securely. The Joint Task Force-Global Network Operations (now CYBERCOM) directive restricting the use of removable media for such transfers[28] was a necessary measure to mitigate real vulnerabilities and protect C2 networks. However, no reasonable alternatives were offered except exceptions to policy to allow limited air-gap transfers via CDs or DVDs. DOD components are establishing institutional means to conduct high-risk data transfers, such as File Sanitization Tool kiosks,[29] but these capabilities still rely on

external media devices and must be locally fielded and managed.[30] Re-enabling the use of removable media with such solutions is solving the wrong problem—the use of removable media for cross-domain transfers proliferated because networks and systems lack organic CDS capabilities. As Admiral Keating noted when he was the commander of U.S. Northern Command, the military must be careful about buying new technology as a quick solution because countering threats also involves culture and processes.[31]

A better short term approach for unstructured data (or data that is not time-critical) is an expansion of AMHS or an adapted parallel capability designed for high-speed, reliable, and secure cross-domain transfers. AMHS already incorporates the prerequisite system functions necessary to operate in multiple security domains simultaneously. The National Gateway Center at Fort Detrick ensures interoperability with allies, coalition partners, non-DOD agencies, and other non-DOD U.S. and foreign organizations. It has data transformation functions, data integrity controls, and synchronization mechanisms. The means by which AMHS delivers official message traffic to other domains based on security labeling can be extended to facilitate deterministic transfers of files and other data packages with high integrity and non-repudiation.[32] Information assurance controls already exist for malware scanning. AMHS implements role-based access and confidentiality measures through the DOD public key infrastructure and is Protection Level 3[33] certified. Role functions could be extended to assure two-person review of packages before transfer, and the current releaser role could be tailored for approvals by foreign disclosure officers in standard operations, or personally by commanders in exigent circumstances. Users interact with

AMHS via web clients, eliminating the need for proximity to custom workstations to conduct transfers. No removable media would be involved in these automated exchanges, which eliminates that vector from the vulnerability array of the system. If used in conjunction with MLS data stores, the movement of data from one domain to another could be on-demand and fully automated. Although a comprehensive capacity and performance study is necessary to ensure high availability, the fundamental subsystems for cross-domain interoperability are already present.

Long Term Strategy

Enterprise Cross-Domain Services

The DOD objective capability is enterprise-level cross-domain services that operate within a service-oriented architecture. CDS on the Global Information Grid (GIG) would no longer be point-to-point interfaces; rather, they would be discoverable based on solution attributes and remotely invoked by service calls made by C2 systems on behalf of the user. The Defense Information System Agency (DISA) and Defense Intelligence Agency (DIA) will consolidate CDS into cross-domain service centers, coupled together on a common services bus, and connected to reliable high bandwidth fast transport. The system will deliver messages to the desired destinations seamlessly by determining the best device and location to perform the cross-domain service.[34] Delivery may be synchronous or asynchronous, depending on mission requirements and data pedigree. The cross-domain enterprise will also provide information discovery, collaboration, and information technology management across security domains to support core C2 functions.[35]

The DOD and IC have already achieved two critical steps towards the goal of enterprise cross-domain services. The first step was the establishment of the Unified

Cross-Domain Management Office (UCDMO) to provide centralized coordination and oversight of all cross-domain initiatives across all U.S. Government agencies, led by the Director of the National Security Agency. The UCDMO is not a new organization, but rather a jurisdictional office which manages CDS investments, addresses cross-domain functional needs, and manages a CDS roadmap for the interagency environment.[36] The second step was the creation of the UCDMO Cross-Domain Solutions Overlay. It is a list of cross-domain technologies that are already in place somewhere, have a government sponsor and at least a three year lifecycle support agreement. With these governing structures and mandates, the UCDMO has clarified the paths to enterprise CDS standards which will lead to CDS interoperability at the joint and interagency levels. Interoperability at the intergovernmental and multinational levels will subsequently evolve from these efforts. To ensure interoperability with future enterprise cross-domain services from 2015 to 2020, DOD components must adhere to the UCDMO Cross-Domain Solutions Overlay not only in CDS development, but also in designing overarching C2 capabilities that have cross-domain requirements.[37]

Domain Convergence

The emerging concept of domain convergence is the antithesis of CDS architectures. In a domain convergence environment, encrypted data elements of all classifications traverse common network infrastructure. This differs from a converged network, where different services use common infrastructure. It is also different from tunneling solutions or encrypted multiplexing, where classified networks are encrypted, multiplexed, sent along bulk (usually unclassified) transport, de-multiplexed, and finally unencrypted at the perimeter of the target security domain enclave. On a converged network, all the packets travel together end-to-end. Endpoint devices can decrypt data

elements based on the operating environment they are within. For example, a trusted workstation connected to a domain-converged portion of the GIG in an unclassified facility would only be able to decrypt and process NIPRNet packets. In a Secret facility, trusted workstations could access the NIPRNet and SIPRNet data link layers on the same transport medium. Interface subsystems at the workstation control what packets are visible to the network adapter, control the labeling and encryption of outbound packets based on classification, and negotiate key management for access. Packet filtering may be used at edge devices to prevent packets with classifications exceeding that of the enclave from entering internal network segments, unless end-to-end encryption schemes make such screening unnecessary. Domain convergence is highly dependent on extensible network protocols like Internet Protocol version 6, robust encryption algorithms, and significant computing power at edge devices. Demonstrations of this technology are likely in the next 7-8 years, but domain convergence for C2 systems of record is not likely until 2020 and beyond.

The Costs of Doing Business

The UCDMO has been efficacious in providing uniform solutions and at less overall cost to the government.[38] The DOD Chief Information Officer directed all Components to form their own Cross Domain Support Element (CDSE) to be the focal point for all cross-domain related activities in their respective organizations.[39] Despite these efforts, there is no shortage of impediments to suitable CDS for C2 at all levels. Critiques and criticisms of existing CDS come from all disciplines and communities. Notwithstanding the common shortfalls in C2 system design which impose requirements back on CDS developers, there are other legitimate considerations for future interoperability between security domains.

Complex Systems Are Expensive

Cross-domain solutions are some of the most expensive computing systems in today's marketplace. The vast corporate resources required to design, manufacture and certify trusted guards prohibits all but the largest information technology providers from undertaking CDS production. Certification itself is a costly proposition. The Defense Information Assurance/Security Accreditation Working Group (DSAWG) approves CDS for Secret and Below Interoperability (SABI) based on compliance with nine NSA guard Security Requirements (SR 1-9) and Risk Decision Authority Criteria (RDAC). For Top Secret and Below Interoperability (TSABI), CDS must meet Intelligence Community Directive 503 guidance.[40] After approval, the employing organization must provide resources to integrate the CDS with the overall capability. Organizations usually keep contract staff on hand for specialized maintenance and rule set adjustments. Enterprise-level CDS can cost hundreds of thousands of dollars to procure and field. Distributed CDS solutions integrated into new or existing systems will impose even greater outlays.

Security Still Trumps All

Cross-domain solutions do not diminish physical and communications security requirements. The security domains connected by CDS must still meet the statutory and regulatory requirements for restricting physical access and preventing unauthorized interceptions of data at rest and in transit. MSL and MLS systems take a system-high approach to physical and communications security measures. Even if the delivery of data in a COP view is properly tailored for each user's level of authorization, the environment must meet the security requirements of the highest possible classification of data accessed and viewed by users. Likewise, the supporting infrastructure for a

trusted computing environment must adhere to the most restrictive security policies for the domains it connects with.

Executive Order 13526 Reform

The appearance of military computer systems and the evolution of physical security enclaves occurred in the context of Eisenhower's Executive Order 10290. Today's networks inherit their genetic disposition to the 1958 ARPA scheme of physical data segregation by classification. Should the current system for classifying, safeguarding, and declassifying national security information be reconstructed? Many DOD and IC leaders voice concern about the relevancy of the current classification levels. A 2006 Government Accountability Office study found that DOD organizations manage classification and declassification poorly, especially among originators.[41] However, it is unlikely that more implicit terms than "damage," "serious damage," and "exceptionally grave damage"[42] would make much of a difference, since less than 1 percent of the classification decisions made in DOD are original.[43] Even if information security mechanisms could provide adequate security in a purely role-based environment (that is, if classifications were eliminated altogether), the burden of managing complex role memberships throughout the DOD enterprise would be paralyzing. Some general categorizations of information are necessary to make personnel management (clearance and vetting), classification procedures, and information system design practical. Because the potential user base is so diverse, approaches that rest on the principle that a user requesting access should be known a priori are generally ineffective. Instead, the critical issue in such an environment is not "Who exactly is this requester," but "Do I trust this requester to share my resource?" The properties or attributes possessed by the requesting users, such as clearance, are

more relevant to characterizing them and determining whether or not they should be trusted.[44] Adjusting the current classifications and dissemination controls to better reflect defense operating environments would be more pragmatic than a reform of the entire system, such as the recent addition of the Controlled Unclassified Information (CUI) category in Executive Order 13556.[45]

Conclusion

Commanders have operated in multiple security domains since the advent of national security classification structures and C2 systems. Planning, execution, and control in JIIM environments demands the movement of information between the security domains of all participants. In the short term, CDS can facilitate the requisite transfers for systems designated to operate at multiple security levels or with multilevel security, but three short term measures are still necessary. First, capability developers must represent cross-domain requirements properly during system analysis and design. Second, interoperability certification processes in the DOD components must require explicit identification of cross-domain requirements, and architectures must reflect these operational requirements so the necessary resource flows are incorporated into system design. Third, MSL systems with extensible cross-domain capabilities, such as AMHS, should expand their functions to provide cross-domain capability to commanders until multilevel security solutions become more prevalent and less costly. In the long term, capability developers should incorporate enterprise cross-domain services into objective architectures, in anticipation of DISA and DODIIS provisioning fast, reliable, and centralized guard farms. In addition, research and development efforts beyond the 2013 Future Years Defense Program call for domain convergence solutions which

reduce infrastructure, increase interoperability, and give greater flexibility in command and control.

Endnotes

[1] David Pearson, *WWMCCS Evolution* (Maxwell Air Force Base, AL: Air University), 192-193.

[2] Office of the Deputy Chief Management Officer, "Joint Capability Areas," U.S. Department of Defense, http://dcmo.defense.gov/products-and-services/business-enterprise-architecture/9.0/reports/bealist_jointcapabilityarea_na.htm (accessed February 26, 2013).

[3] U.S. Defense Intelligence Agency Chief Information Officer, "Information Management Strategic Vision 2012-2017," (Bolling AFB, MD: U.S. Defense Intelligence Agency), 3.

[4] NATO/OTAN HQ Allied Air Command, "The Afghanistan Mission Network," http://www.airn.nato.int/focus_areas/mjo/articles/mjo0310.htm (accessed December 1, 2012).

[5] Noel Brinkerhoff, "8 Extremely Little-Known Corners of the U.S. Intelligence Network...and 4 More," June 4, 2009, http://www.allgov.com/news/top-stories/8-extremely-little-known-corners-of-the-us-intelligence-networkand-4-more?news=838962 (accessed February 26, 2013).

[6] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: W. W. Norton & Company, 2004), 10-11.

[7] Charles Maney, *Security Issues When Data Traverses Information Domains: Do Guards Effectively Address the Problem?* (Bethesda, MD: SANS Institute, May 2004): 3-4.

[8] Joint Interoperability Test Command, "AMHS/DMS System Description, Joint GCCS Interoperability," http://jitc.fhu.disa.mil/gccsiop/interfaces/amhsdms.pdf (accessed December 1, 2012).

[9] Chairman of the Joint Chiefs of Staff, "Policy and Procedures for Management and Use of United States Message Text Formatting," CJCSI 6241.01E (Washington, DC: Chairman of the Joint Chiefs of Staff, August 13, 2012), 1.

[10] Henry S. Kenyon, "Global Command and Control Rebooted," *Signal Online* (November 2009), http://www.afcea.org/content/?q=node/2108 (accessed December 1, 2012).

[11] U.S. Department of Defense Chief Information Officer, "The DOD Architecture Framework version 2.02," http://cio-nii.defense.gov/sites/dodaf20/background.html (accessed December 1, 2012).

[12] U.S. Department of Defense Chief Information Officer and U.S. Intelligence Community Chief Information Officer, "Use of Unified Cross Domain Management Office (UCDMO) Baseline Cross Domain Solutions (CDS)," memorandum for DOD Components, Washington, DC, December 1, 2011.

[13] United States Army, “Flat Network Analysis System,” *2008 Army Posture Statement Information Papers* (Feb 2008), http://www.army.mil/aps/08/information_papers/transform/Flat_Network_Intelligence_Access.html (accessed December 1, 2012).

[14] Robert K. Ackerman, “Army Intelligence Consolidates Data”, *Signal Magazine* (October 2005): 20.

[15] Steven Boutelle and Charles Pizzutelli, “First Digital Division Implementation,” *Army RD&A* (September-October 1998): 5-7.

[16] Michael Rauhut, “From Experimental Force to Deployable Unit: The Transition of the 4th Infantry Division (Mechanized),” *Army* (June 2002): 66-70.

[17] Harold Greene and Robert Mendoza, “Lessons Learned From Developing the ABCS 6.4 Solution,” *Defense Acquisition Review Journal* (April 2005): 198-201.

[18] Jane’s Information Group, “C4ISR and Mission Systems: Joint and Common Equipment,” *Jane’s* (Englewood, CA: IHS Jane’s, 2011): 372.

[19] Joint Requirements Oversight Council, “Blue Force Tracking,” JROCM 161-03 (Washington, DC: The Joint Staff, August 13, 2003).

[20] “New Platform for Battle Command,” *Military Information Technology* 15, Issue 1 (February 2011): 6-10.

[21] Harry Greene, Larry Stotts, Ryan Paterson, and Janet Greenberg, “Command Post of the Future: Successful Transition of a Science and Technology Initiative to a Program of Record,” *Defense Acquisition Review Journal* 17, Issue 1 (January 2010): 6-9.

[22] Penny Myer and Sue Patterson, “Providing a Multilevel Secure Solution for the Rapidly Expanding World of C4I,” *Sea Systems Command San Diego Biennial Review* (2003): 57-60.

[23] John J. Falbo and Christopher J. Newcomb, *Lessons Learned From an Afloat Installation of an Ashore Command and Control System* (Monterey, CA: Naval Postgraduate School, September 2005), 15-29.

[24] Office of the Director, Operational Test and Evaluation, “Air Operations Center – Weapon System,” *FY2011 Annual Report* (Washington, DC: U.S. Department of Defense, December 2011), 191-193.

[25] Information Directorate, AFRL/IF, “DoDIIS Trusted Workstation 3.2 Installed at Multiple Sites,” (May 2006), http://www.wpafb.af.mil/news/story.asp?id=123033821 (accessed February 26, 2013).

[26] Barry Rosenberg, “Agile Intelligence is the Name of the Game at DIA,” *Defense Systems* 5, Issue 8, (April 2011): 16-18.

[27] Chairman of the Joint Chiefs of Staff, “Net Ready Key Performance Parameter (NR KPP),” CJCSI 6212.01F (Washington, DC: Chairman of the Joint Chiefs of Staff, March 21, 2012), Enclosure D.

[28] Joint Task Force – Global Network Operations, "Removable Flash Media Device Implementation," CTO 10-004A (Fort Meade, MD: Joint Task Force – Global Network Operations, February 16, 2010).

[29] U.S. Department of the Army, "HQDA Command Directive for the Continued Ban of USB Flash Media on Army Networks," ALARACT 137/2010 (Washington, DC: Headquarters, Department of the Army, 111505Z May 10).

[30] Tresys Technology, "Enabling Mobile and Portable Media for Use in Mission Critical Operations," http://www.tresys.com/study_7.pdf (accessed December 16, 2012).

[31] Henry S. Kenyon, Robert K. Ackerman, and Maryann Lawlor, "Creating an Information-Sharing Culture for Homeland Security," *Signal* 58, Issue 8 (April 2005): 71.

[32] Chairman of the Joint Chiefs of Staff, "The Defense Message System and Associated Legacy Message Processing Systems," CJCSI 5721.01E (Washington, DC: Chairman of the Joint Chiefs of Staff, August 13, 2010), 2.

[33] Director of Central Intelligence, "Protecting Sensitive Compartmented Information Within Information Systems," DCI Directive 6/3 (Washington, DC: Director of Central Intelligence, June 5, 1999), 4.B. Protection Level 3 (PL3) is a confidentiality requirement defined by the Director of Central Intelligence for systems accessed by users cleared to a level at least equal to the highest data, where not all users have formal access approval to all data, and where need to know considerations do not contribute to access control decisions.

[34] Bassam S. Farroha, Melina M. Whitfield, and Deborah L. Farroha, "Enabling Information Sharing through Cross Domain Solutions: Architecting the Enterprise," (Chantilly, VA: Unified Cross Domain Management Office, 2009), 10-11.

[35] U.S. Department of Defense Chief Information Officer, "Initial Capabilities Document for Cross Domain Enterprise, version 0.8," (Washington, DC: U.S. Department of Defense Chief Information Officer, December 8, 2010), 6-17.

[36] U.S. Department of Defense Chief Information Officer and U.S. Intelligence Community Chief Information Officer, "Establishment of a Department of Defense (DOD)/Intelligence Community (IC) Unified Cross Domain Management Office (CDMO)," memorandum for DOD Components, Washington, DC, July 10, 2006.

[37] Unified Cross Domain Management Office, "Cross Domain Solution Overlay," (Chantilly, VA: Unified Cross Domain Management Office, November 1, 2012), 6-8.

[38] U.S. Department of Defense Chief Information Officer and U.S. Intelligence Community Chief Information Officer, "Establishment of a Department of Defense (DOD)/Intelligence Community (IC) Unified Cross Domain Management Office (CDMO)," memorandum for DOD Components, Washington, DC, July 10, 2006.

[39] U.S. Department of Defense Chief Information Officer, "Cross Domain Support Element (CDSE) Responsibilities," memorandum for DOD Components, Washington, DC, October 11, 2011.

[40] Steve Welke, “Certification and Accreditation (C&A) Basics,” *Journal of Software Technology* 13, No 2 (June 2010): 5-8.

[41] U.S. Government Accountability Office, *GAO-06-706, Managing Sensitive Information: DOD Can More Effectively Reduce the Risk of Classification Errors* (Washington, DC: U.S. Government Accountability Office, June 2006), 5.

[42] Executive Order 13526: Classified National Security Information, *Federal Register* 75, no. 705, (January 5, 2010): 707-708.

[43] U.S. Government Accountability Office, *GAO-06-706, Managing Sensitive Information: DOD Can More Effectively Reduce the Risk of Classification Errors* (Washington, DC: U.S. Government Accountability Office, June 2006), 7.

[44] Jing Jin, “Assured Information Sharing For Ad-Hoc Collaboration,” (Charlotte, NC: The University of North Carolina, 2009), 3-4.

[45] Executive Order 13556: Controlled Unclassified Information, *Federal Register* 75, no. 68675, (November 9, 2010): 68675-68677.